Research Article

Claude Carlet, David Joyner*, Pantelimon Stănică and Deng Tang

Cryptographic properties of monotone Boolean functions

DOI: 10.1515/jmc-2014-0030
Received September 2, 2014; revised December 28, 2015; accepted December 30, 2015

Abstract: We prove various results on monotone Boolean functions. In particular, we prove a conjecture proposed recently, stating that there are no monotone bent Boolean functions. Further, we give an upper bound on the nonlinearity of monotone functions in odd dimension, we describe the Walsh–Hadamard spectrum and investigate some other cryptographic properties of monotone Boolean functions.

Keywords: Boolean functions, bent and monotone functions, Walsh–Hadamard spectrum, algebraic immunity

MSC 2010: 06E30, 94C10, 94A60, 11T71, 05E99

Communicated by: Carlo Blundo

1 Introduction

Let $\mathbb{F}_2$ be the prime field of characteristic 2 and let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called a Boolean function on n variables. The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$.

Any element $\mathbf{x} \in \mathbb{F}_2^n$ can be written as an n-tuple $(x_1, \dots, x_n)$, where $x_i \in \mathbb{F}_2$ for all $i = 1, \dots, n$. We let the *support* $\mathrm{supp}(\mathbf{x})$ be the set of all positions i where $x_i = 1$. The *(Hamming) weight* of $\mathbf{x} \in \mathbb{F}_2^n$ is denoted by $w_H(\mathbf{x})$ and equals $\sum_{i=1}^n x_i$ (the Hamming weight of a function is the weight of its truth table, more precisely of its output vector, that is, the size of its support, see below). The sets of integers, real numbers and complex numbers are denoted by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, respectively. The addition over all these sets, as well as on $\mathbb{F}_2^n$, is denoted by '+'. We denote the (vector) *complement* by $\overline{\mathbf{x}} = (x_1 + 1, \dots, x_n + 1)$, and the (Boolean function) *complement* by $\overline{f}(\mathbf{x}) = f(\mathbf{x}) + 1$, for $f \in \mathcal{B}_n$. If we define the *union* as

$$(f \vee g)(\mathbf{x}) = f(\mathbf{x}) + g(\mathbf{x}) + f(\mathbf{x})g(\mathbf{x})$$

then the *double complement* operation, $f(\mathbf{x}) \mapsto \overline{f}(\overline{\mathbf{x}})$, has the following properties:

$$\overline{f}(\overline{\mathbf{x}}) \vee \overline{g}(\overline{\mathbf{x}}) = \overline{fg}(\overline{\mathbf{x}}), \quad \overline{f \vee g}(\overline{\mathbf{x}}) = \overline{f}(\overline{\mathbf{x}})\overline{g}(\overline{\mathbf{x}})$$

(recall that $fg(\mathbf{x}) = f(\mathbf{x})g(\mathbf{x})$). If $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ are two elements of $\mathbb{F}_2^n$, we denote the *inner product* and the *intersection*, respectively, by

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n, \quad \mathbf{x} * \mathbf{y} = (x_1y_1, x_2y_2, \dots, x_ny_n).$$

Claude Carlet, Deng Tang: LAGA, Department of Mathematics, University of Paris 8, Saint-Denis cedex 02, France, e-mail: claude.carlet@univ-paris8.fr, dtang@foxmail.com
***Corresponding author: David Joyner:** Mathematics Department, United States Naval Academy, Annapolis, MD 21402, USA, e-mail: wdj@usna.edu
Pantelimon Stănică: Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5216, USA, e-mail: pstanica@nps.edu

We define the *union* $\mathbf{x} \vee \mathbf{y}$ to be the vector in $\mathbb{F}_2^n$ whose ith component is 0 if and only if $x_i = y_i = 0$. In particular, $\mathrm{supp}(\mathbf{x} \vee \mathbf{y}) = \mathrm{supp}(\mathbf{x}) \cup \mathrm{supp}(\mathbf{y})$. For $\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$, we define the following partial order on $\mathbb{F}_2^n$:

$$\mathbf{u} \preceq \mathbf{v} \quad \text{if and only if} \quad u_i \le v_i \text{ for every } i.$$

The cardinality of the set S is denoted by $|S|$.

For a detailed study of Boolean functions we refer the reader to Carlet [2, 3] and Cusick and Stănică [7]. For the reader's convenience, we recall some basic notions below.

Any $f \in \mathcal{B}_n$ can be expressed in *algebraic normal form* (ANF) as

$$f(x_1, x_2, \ldots, x_n) = \sum_{\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_{\mathbf{a}} \Big(\prod_{i=1}^{n} x_i^{a_i} \Big),$$

for some coefficients $\mu_{\mathbf{a}} = \mu_a(f) \in \mathbb{F}_2$. Any term of the form $\prod_{i=1}^n x_i^{a_i}$ is called a *monomial*. The ANF of any Boolean function satisfies $\mu_{\mathbf{a}} = \sum_{\mathbf{x}\preceq\mathbf{a}} f(\mathbf{x})$ and $f(\mathbf{x}) = \sum_{\mathbf{a}\preceq\mathbf{x}} \mu_{\mathbf{a}}$.

The algebraic degree of f, $\deg(f)$, equals $\max_{\mathbf{a}\in\mathbb{F}_2^n}\{w_H(\mathbf{a}) \mid \mu_{\mathbf{a}} \neq 0\}$. Boolean functions having algebraic degree at most 1 are *affine functions*. For any two functions $f, g \in \mathcal{B}_n$, we define the *(Hamming) distance*

$$d(f, g) = \big|\{\mathbf{x} \mid f(\mathbf{x}) \neq g(\mathbf{x}),\ \mathbf{x} \in \mathbb{F}_{2^n}\}\big|.$$

The *support* of a Boolean function f is the set $\mathrm{supp}(f) = \{\mathbf{x} \mid f(\mathbf{x}) = 1\}$.

The (unnormalized) *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at any point $\mathbf{u} \in \mathbb{F}_2^n$ is defined by

$$W_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}. \tag{1.1}$$

The multiset $[W_f(\mathbf{u}) \mid \mathbf{u} \in \mathbb{F}_2^n]$ is called the *Walsh–Hadamard spectrum* of function f. The *nonlinearity* of f is its distance from the set A_n of all n-variable affine functions, that is,

$$\mathrm{nl}(f) = \min_{g\in A_n} d(f, g).$$

A function $f \in \mathcal{B}_n$ is a *bent function* if the Walsh–Hadamard transform (1.1) has constant absolute value $2^{n/2}$ (which is possible only for n even). It is well known that $f \in \mathcal{B}_n$ is bent if and only if its nonlinearity achieves the optimum $2^{n-1} - 2^{n/2-1}$. Bent functions[1] hold an interest among researchers in this area since they have maximum Hamming distance from the set of all affine Boolean functions and have very nice combinatorial properties, used in many domains such as sequences, cryptography and designs. Several classes of bent functions were constructed by Rothaus [16], Dillon [9], Dobbertin [10], and Carlet [1]. If f is bent, then there exists a Boolean function $\tilde{f}$ such that $W_f(\mathbf{u}) = 2^{n/2}(-1)^{\tilde{f}(\mathbf{u})}$ for every $\mathbf{u} \in \mathbb{F}_2^n$. This function, called the *dual of* f, is bent as well [9].

A non-zero vector $\mathbf{a}$ is called a *linear structure* for a Boolean function f if the derivative

$$D_a f(\mathbf{x}) = f(\mathbf{x}) + f(\mathbf{x} + \mathbf{a})$$

(sum calculated in $\mathbb{F}_2$) is constant for any $\mathbf{x}$. It is known [9, 16] that bent functions are those functions whose derivatives are balanced, and so bent functions do not have any non-zero linear structure.

The sum $\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{z})}$ is the *crosscorrelation* of f and g at $\mathbf{z}$. The *autocorrelation* of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$. The multiset $[\mathcal{C}_f(\mathbf{u}) \mid \mathbf{u} \in \mathbb{F}_2^n]$ is called the autocorrelation spectrum of the function f.

For any $f \in \mathcal{B}_n$, a non-zero function $g \in \mathcal{B}_n$ is called an *annihilator* of f if fg is null, and the *algebraic immunity* of f, denoted by $\mathcal{AI}(f)$, is the minimum value of d such that f or $f + 1$ admits an annihilator of

1 Bent functions were first studied by Rothaus in the 1960s, although his paper was not published until ten years later, in [16]. Their first appearance was in a preprint of Dillon in 1972, and then, with more details, a few years later in his thesis [9].

degree d (see [13]). It is known [5] that the algebraic immunity of an n-variable Boolean function is bounded above by $\lceil \frac{n}{2} \rceil$.

A Boolean function f is *monotone* (increasing) if whenever $\mathbf{u} \preceq \mathbf{v}$, then $f(\mathbf{u}) \leq f(\mathbf{v})$. It is easy to see that any monomial Boolean function is monotone. Other examples are the strict (resp. large) *majority functions* $M \in \mathcal{B}_n$ (and more generally the functions whose supports are the sets of vectors of Hamming weights bounded by some number from below). The value of $M(\mathbf{x})$ is 0 if and only if the Hamming weight of $\mathbf{x}$ is strictly less than $n/2$ (respectively, it is smaller than or equal to $n/2$).

If f is a monotone Boolean function (or more generally any Boolean function), we define the *least (vector) support set* $\Gamma = \Gamma_f \subseteq \mathrm{supp}(f) \subseteq \mathbb{F}_2^n$, consisting of all vectors in $\mathrm{supp}(f)$ that are smallest in the partial ordering $\preceq$. An *atomic* (monomial) monotone function is one for which $|\Gamma_f| = 1$.

Recall that $\mathbf{v}_1 \vee \mathbf{v}_2$ denotes the vector with component 0 if and only if both the components of $\mathbf{v}_1, \mathbf{v}_2$ are 0 in that position. With a set of vectors $\{\mathbf{v}_i\}_i$ fixed, we set

$$E_{i_1 i_2 \ldots i_k} = \{\mathbf{u} \in \mathbb{F}_2^n \mid \mathbf{u} * \mathbf{v}_{i_1 i_2 \ldots i_k} = \mathbf{0}\}, \tag{1.2}$$

where we use the notation

$$\mathbf{v}_{i_1 i_2 \ldots i_k} = \bigvee_{j=1}^{k} \mathbf{v}_{i_j} = \mathbf{v}_{i_1} \vee \mathbf{v}_{i_2} \vee \cdots \vee \mathbf{v}_{i_k}.$$

Recall the Kronecker delta function $\delta_S(\mathbf{u})$ with $\delta_S(\mathbf{u}) = 1$ for $\mathbf{u} \in S$, and $\delta_S(\mathbf{u}) = 0$ otherwise. If $S = \{\mathbf{0}\}$ we will drop the subscript S, and write $\delta(\mathbf{u})$.

For $\mathbf{v} \in \mathbb{F}_2^n$, we use the usual multi-index notation $\mathbf{x}^{\mathbf{v}}$ for the product of variables, with indices running through the non-zero positions of $\mathbf{v}$:

$$\mathbf{x}^{\mathbf{v}} = \prod_{i \in \mathrm{supp}(\mathbf{v})} x_i.$$

Monotone Boolean functions are important, since they have many applications in voting theory, reliability theory, hypergraphs, etc. (cf. Crama and Hammer [6]). So, it is natural to inquire about their cryptographic properties as well. It is the purpose of this paper to look at some of the main cryptographic properties of a Boolean function, namely, (maximum) nonlinearity, balancedness and algebraic immunity, in the context of monotone Boolean functions. In particular, we will show that there are no monotone bent functions, using Walsh transform computations (see Section 4 below).

2 Preliminaries

We survey some properties of a monotone Boolean function (we shall not use many of them, but they are interesting, nonetheless). We shall follow mostly [4].

Recall that the Hasse diagram, P_n, is the directed graph whose vertex (node) set is $\mathbb{F}_2^n$, and edges $(\mathbf{v}, \mathbf{w})$ if $\mathbf{v} \preceq \mathbf{w}$ and $w_H(\mathbf{w}) = w_H(\mathbf{v}) + 1$. A closure $C \subseteq G$ of a directed graph $G = (V, E)$ is the set of nodes without any outgoing edges (if $a \in C$ and $(a, b) \in E$, then $b \in C$). It was shown in [4] that the set of closures in P_n is in one-to-one correspondence with the set of monotone functions on $\mathbb{F}_2^n$.

The following interesting theorem on the ANF of a monotone Boolean function was proved in [4], and we shall use it throughout the paper.

Theorem 2.1 (Celerier et al. [4]). *Let f be a monotone function whose least vector support set is $\Gamma \subset \mathbb{F}_2^n$. Then*

$$f(\mathbf{x}) = 1 + \prod_{\mathbf{v} \in \Gamma} (1 + \mathbf{x}^{\mathbf{v}}).$$

In terms of complements, this can be written

$$f(\mathbf{x}) = \overline{\prod_{\mathbf{v} \in \Gamma} \overline{\mathbf{x}^{\mathbf{v}}}}.$$

Remark 2.2. Given any Boolean function f, the function $f'(\mathbf{x}) = 1 + \prod_{\mathbf{v}\in \mathrm{supp}(f)}(1+\mathbf{x}^{\mathbf{v}})$ takes value 1 at $\mathbf{x}$ if and only if there exists $\mathbf{v} \in \mathrm{supp}(f)$ such that $\mathbf{v} \preceq \mathbf{x}$. Hence, f' is the least monotone function such that $f \le f'$ (and f is monotone if and only if $f = f'$). Let Γ be its least vector support set, then $f'(\mathbf{x}) = 1 + \prod_{\mathbf{v}\in\Gamma}(1+\mathbf{x}^{\mathbf{v}})$, since $\mathbf{v} \preceq \mathbf{w} \Rightarrow 1 + \mathbf{x}^{\mathbf{v}} \le 1 + \mathbf{x}^{\mathbf{w}} \Rightarrow (1+\mathbf{x}^{\mathbf{v}})(1+\mathbf{x}^{\mathbf{w}}) = 1 + \mathbf{x}^{\mathbf{v}}$. Note that f and f' have the same Γ and we can see that if we apply to f' the same transformation again, we get the same function f'. Note also that if $\mathbf{v} \in \Gamma$ then $\mathbf{x}^{\mathbf{v}}$ necessarily appears in the ANF of f (and f') since the coefficient of $\mathbf{x}^{\mathbf{v}}$ in this ANF is $\sum_{\mathbf{x}\preceq\mathbf{v}} f(\mathbf{x}) = f(\mathbf{v}) = 1$.

Let f be a monotone Boolean function of least vector support set $\Gamma = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$. For any $1 \le s \le m$, we denote

$$\Gamma_{i_1 i_2 \ldots i_s} = \Gamma \setminus \{\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \ldots, \mathbf{v}_{i_s}\}.$$

When $s = 0$, by convention, we set $\Gamma_{i_1 i_2 \ldots i_s} = \Gamma$. Using Theorem 2.1, we easily deduce the following corollary.

Corollary 2.3. *If f is monotone with least vector support set Γ of cardinality m, then*

$$f = \sum_{\substack{0\le s<m \\ 1\le i_1<\cdots<i_s\le n}} \prod_{\mathbf{v}\in\Gamma_{i_1 i_2 \ldots i_s}} \mathbf{x}^{\mathbf{v}}. \tag{2.1}$$

Remark 2.4. It might be tempting to conjecture that $\prod_{\mathbf{v}\in\Gamma} \mathbf{x}^{\mathbf{v}}$ appears in the ANF of the monotone Boolean function f, that is, that all variables occurring in the ANF will occur in a *single* highest degree term of f. This would allow simplifying some proofs given below. However, that happens to be false, in general, since there may be cancellations in equation (2.1). As an example (see [4, Example 4.2]), let $f \in \mathcal{B}_6$ be the monotone function with least support set $\Gamma = \{(1,1,1,1,0,0), (1,1,0,0,1,1), (0,0,1,1,1,1)\}$. The ANF of f is in fact $f(\mathbf{x}) = x_1x_2x_3x_4 + x_1x_2x_5x_6 + x_3x_4x_5x_6$, and so, all variables will occur, but spread out in several monomials.

A similar example, also monotone but in 5 variables, is $g(\mathbf{x}) = x_0x_1x_2x_4 + x_0x_1x_3x_4 + x_0x_2x_3x_4$.

The first example has the additional property that $W_f(\mathbf{u}) \neq 0$ for all $\mathbf{u} \in \mathbb{F}_2^6$. However, this property does not hold for $g \in \mathcal{B}_5$. It appears that $n = 6$ is the smallest dimension for which there exists a monotone homogeneous function having non-zero Walsh–Hadamard spectrum, that is, $W_f(\mathbf{u}) \neq 0$ for all $\mathbf{u} \in \mathbb{F}_2^6$.

Remark 2.5. If $\deg(f) < n$ and there does not exist $\Gamma_1 \subset \Gamma$ such that

$$\bigcup_{\mathbf{v}\in\Gamma} \{x_i \mid i \in \mathrm{supp}(\mathbf{v})\} = \bigcup_{\mathbf{w}\in\Gamma_1} \{x_i \mid i \in \mathrm{supp}(\mathbf{w})\},$$

then the ANF of f lacks a variable. This implies that there is a variable, say x_i, that f does not depend on. Thus, f has a linear structure, since $f(x) + f(x + e_i) = 0$, for all $x \in \mathbb{F}_2$, where e_i is the standard basis vector with 1 in the ith position and 0 elsewhere.

3 Constructions of monotone functions

We note that $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is monotone if and only if the subfunctions $f_j(x_1, \ldots, x_{n-1}) = f(j, x_1, \ldots, x_{n-1})$ $(j = 0, 1)$ are monotone and satisfy $\mathrm{supp}(f_0) \subseteq \mathrm{supp}(f_1)$.

Three elementary examples of secondary constructions of monotone functions (building a monotone function from monotone functions $g_1, \ldots$) are the "double complement" operation

$$g \mapsto \overline{g}(\overline{\mathbf{x}}) = g(x_1 + 1, \ldots, x_n + 1) + 1$$

and the operations $g_1 \cdot g_2 = g_1g_2$ and $g_1 \vee g_2 = g_1 + g_2 + g_1g_2$. Note that the "double complement" operation is involutive (hence, $g \in \mathcal{B}_n$ is monotone if and only if $\overline{g}(\overline{\mathbf{x}})$ is monotone) and exchanges $g_1 \cdot g_2$ and $g_1 \vee g_2$.

It is easy to construct monotone functions using the monomials and the operations of "$\cdot$" and "$\vee$".

According to Theorem 2.1, constructing a monotone function is straightforward: we choose a set Γ of vectors which are non-comparable with respect to $\preceq$ and we define $f(\mathbf{x}) = 1 + \prod_{\mathbf{v}\in\Gamma}(1+\mathbf{x}^{\mathbf{v}})$ (note that if Γ includes vectors which are comparable, then this gives also a monotone function, but the set of minimal elements in $\mathrm{supp}(f)$ is not equal to Γ).

The secondary constructions "$\cdot$" and "$\vee$" are particular cases of a much more general secondary construction, which is easy to show and certainly known (see, for example, [11]).

Theorem 3.1. *Let*

- $f \in \mathcal{B}_n$ *be monotone, and*
- $g_1, \ldots, g_n$ *be n monotone functions (in distinct variables or not).*

Then, denoting $\mathbf{g} = (g_1, \ldots, g_n)$*, the vectorial composition* $f \circ \mathbf{g}$ *(viewed as a function in the union of the variables of* $g_1, \ldots, g_n$*) is a monotone function.*

Proof. When any of the variables of $g_1, \ldots, g_n$ move from value 0 to 1, while the others remain constant, each value of $g_1, \ldots, g_n$ does not decrease since $g_1, \ldots, g_n$ are monotone, and then the value of $f \circ \mathbf{g}$ does not decrease either, since f is monotone. □

Note that this result is very general. The knowledge of any monotone function in n variables and of any set of n monotone functions gives a monotone function in a number of variables which can be larger or smaller than n. So we have here a secondary construction of a nature quite different from common secondary constructions of cryptographic Boolean functions (where the numbers of variables most often increase or at least do not decrease), see, e.g., [2].

Note also that the secondary construction "$\cdot$" is obtained from Theorem 3.1 by taking $f(x_1, x_2) = x_1x_2$ and the secondary construction $\vee$ is obtained by taking $f(x_1, x_2) = x_1x_2 + x_1 + x_2 + 1$ (these two functions are the strict and large majority functions).

We give now examples of specifications of the construction of Theorem 3.1. By taking in Theorem 3.1 the g_i equal to monomials in distinct variables and of the same degree and f equal to any monotone function, we obtain a construction which will be useful below:

Corollary 3.2. *If* f *is monotone, then the function obtained by replacing any monomial* $\mathbf{x}^{\mathbf{v}}$ *by* $\mathbf{x}^{\mathbf{v}}\mathbf{y}^{\mathbf{v}}\mathbf{z}^{\mathbf{v}} \ldots$ *(that is, replacing each* x_i *by* $x_iy_iz_i \ldots$*) in the ANF of* f *is monotone as well.*

By taking the function $f(\mathbf{x})$ to be the m-variable (monotone) function $1 + \delta(\mathbf{x}) = 1 + \prod_{i=1}^{m}(1 + x_i)$ and all functions g_i to be monomials, we have:

Corollary 3.3 (Construction MBF). *Let* $f_i(\mathbf{x}) = 1 + \prod_{\mathbf{v}\in\Gamma_i}(1 + \mathbf{x}^{\mathbf{v}})$ *be monotone Boolean functions in* $\mathcal{B}_n$ *of least support sets* $\Gamma_i = (\mathbf{v}_{ij})_j$*. Let* $m = \max_i|\Gamma_i|$ *and let, for each* j*,* Γ_j^* *denote the multi-set obtained from* Γ_j *padded with enough copies of the zero vector* $\mathbf{0}$ *so that* $|\Gamma_j^*| = m$*. We define* $\hat{f}$ *in* $\mathcal{B}_{kn}$ *by*

$$\hat{f}(\mathbf{x}_1, \ldots, \mathbf{x}_k) = 1 + \prod_{i=1}^{m}\Big(1 + \prod_{j=1}^{k}\mathbf{x}_j^{\mathbf{v}_{ij}}\Big); \quad \mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbb{F}_2^n.$$

Observe that $\hat{f}$ has least support set $\hat{\Gamma} = \{(\mathbf{v}_{1j}, \ldots, \mathbf{v}_{kj})_{j=1,\ldots,m}\}$.

We could certainly take all f_i $(1 \le i \le k)$ to be equal to a monotone function f (depending on independent sets of variables), of least support set $\Gamma = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$, and we can use any order on the k copies of Γ. We set

$$\hat{\Gamma} = \Gamma^{(\sigma)} = \{(\mathbf{v}_{\sigma_1(i)}, \mathbf{v}_{\sigma_2(i)}, \ldots, \mathbf{v}_{\sigma_k(i)}) \mid i = 1, 2, \ldots, m\},$$

where σ_i are permutations on $\{1, 2, \ldots, m\}$. Then

$$\hat{f}(\mathbf{x}_1, \ldots, \mathbf{x}_k) = 1 + \prod_{i=1}^{m}\Big(1 + \prod_{j=1}^{k}\mathbf{x}_j^{\mathbf{v}_{\sigma_j(i)}}\Big)$$

is a monotone Boolean function.

Example 3.4. Let

$$f_1(x_1, x_2, x_3) = 1 + (1 + x_1x_2)(1 + x_1x_3)(1 + x_2x_3) = x_1x_2 + x_1x_3 + x_2x_3 \quad \text{and} \quad f_2(x_4) = x_4$$

be monotone functions in $\mathcal{B}_3$ and $\mathcal{B}_1$, respectively, with least vector support set

$$\Gamma_1 = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\} \quad \text{and} \quad \Gamma_2 = \{(1)\} \text{ (padded to } \Gamma_2' = \{(1), (0), (0)\}),$$

respectively. Then

$$\hat{f}(x_1, x_2, x_3, x_4) = 1 + (1 + x_1x_2x_4)(1 + x_1x_3)(1 + x_2x_3) = x_1x_3 + x_2x_3 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_3x_4$$

is also monotone of least vector support set $\hat{\Gamma} = \{(1, 1, 0, 1), (1, 0, 1, 0), (0, 1, 1, 0)\}$.

4 Some (non)existence results on monotone Boolean functions

4.1 Bent monotone functions

Celerier et al. [4] proposed a conjecture, which is proved next.

Theorem 4.1. *For every even $n \geq 4$, there exists no n-variable monotone bent function.*

Proof. The idea behind the proof is to connect a potential monotone bent Boolean function to the majority function, which is known not to be bent, if $n \geq 4$, thus obtaining a contradiction.

For every f monotone, every $\mathbf{y} \notin \mathrm{supp}(f)$ and every $\mathbf{a} \in \mathbb{F}_2^n$, we have

$$\sum_{\mathbf{x} \preceq \mathbf{y}} (-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} = \sum_{\mathbf{x} \preceq \mathbf{y}} (-1)^{\mathbf{a}\cdot\mathbf{x}} = \begin{cases} 2^{w_H(\mathbf{y})} & \text{if } \mathbf{a} \preceq \overline{\mathbf{y}}, \\ 0 & \text{otherwise,} \end{cases}$$

where $\overline{\mathbf{y}}$ is the bitwise complement of $\mathbf{y}$. Indeed, the set $\{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x} \preceq \mathbf{y}\}$ is a vector space and its dual is $\{\mathbf{a} \in \mathbb{F}_2^n \mid \mathbf{a} \preceq \overline{\mathbf{y}}\}$. We know, according to the Poisson summation formula (see [1, Lemma 1], [2, p. 275]; see also [7, p. 8] and [12, Chapter 5, Lemma 2], for some particular cases) that

$$\sum_{\mathbf{x} \preceq \mathbf{y}} (-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} = 2^{w_H(\mathbf{y})-n} \sum_{\mathbf{a}+\mathbf{u} \preceq \overline{\mathbf{y}}} W_f(\mathbf{u}).$$

If f is bent, we have then

$$\sum_{\mathbf{a}+\mathbf{u} \preceq \overline{\mathbf{y}}} (-1)^{\widetilde{f}(\mathbf{u})} = \begin{cases} 2^{n/2} & \text{if } \mathbf{a} \preceq \overline{\mathbf{y}}, \\ 0 & \text{otherwise.} \end{cases}$$

This implies that $\overline{\mathbf{y}}$ has weight at least $n/2$ (i.e. $\mathbf{y}$ has weight at most $n/2$) for every $\mathbf{y} \notin \mathrm{supp}(f)$. Moreover, if $\mathbf{y} \notin \mathrm{supp}(f)$ has weight $n/2$ then $\widetilde{f}$ is identically null on $\{\mathbf{u} \in \mathbb{F}_2^n \mid \mathbf{u} \preceq \overline{\mathbf{y}}\}$.

For every $\mathbf{y} \in \mathrm{supp}(f)$ and every $\mathbf{a} \in \mathbb{F}_2^n$, we have

$$\begin{aligned} \sum_{\mathbf{x} \in \mathbb{F}_2^n, \mathbf{y} \preceq \mathbf{x}} (-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} &= \sum_{\mathbf{x} \in \mathbb{F}_2^n, \overline{\mathbf{x}} \preceq \overline{\mathbf{y}}} (-1)^{1+\mathbf{a}\cdot\mathbf{x}} = \sum_{\mathbf{x} \preceq \overline{\mathbf{y}}} (-1)^{1+\mathbf{a}\cdot\overline{\mathbf{x}}} \\ &= \begin{cases} (-1)^{1+w_H(\mathbf{a})}\, 2^{n-w_H(\mathbf{y})} & \text{if } \mathbf{a} \preceq \mathbf{y}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

The set $\{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{y} \preceq \mathbf{x}\}$ equals $(1, \ldots, 1) + \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x} \preceq \overline{\mathbf{y}}\}$ and $\{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x} \preceq \overline{\mathbf{y}}\}$ is a vector space whose dual equals $\{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x} \preceq \mathbf{y}\}$. According to the Poisson summation formula, we have then

$$\begin{aligned} \sum_{\mathbf{x} \in \mathbb{F}_2^n, \mathbf{y} \preceq \mathbf{x}} (-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} &= 2^{-w_H(\mathbf{y})}(-1)^{w_{H(\mathbf{a})}} \sum_{\mathbf{a}+\mathbf{u} \preceq \mathbf{y}} (-1)^{w_H(\mathbf{u})} W_f(\mathbf{u}) \\ &= 2^{n/2-w_H(\mathbf{y})} \sum_{\mathbf{a}+\mathbf{u} \preceq \mathbf{y}} (-1)^{w_H(\mathbf{a})+w_H(\mathbf{u})+\widetilde{f}(\mathbf{u})}. \end{aligned}$$

Thus

$$\sum_{\mathbf{a}+\mathbf{u} \preceq \mathbf{y}} (-1)^{1+w_H(\mathbf{u})+\widetilde{f}(\mathbf{u})} = \begin{cases} 2^{n/2} & \text{if } \mathbf{a} \preceq \mathbf{y}, \\ 0 & \text{otherwise.} \end{cases}$$

This implies that $\mathbf{y}$ has weight at least $n/2$ for every $\mathbf{y} \in \mathrm{supp}(f)$. Moreover, if $\mathbf{y} \in \mathrm{supp}(f)$ has weight $n/2$ then $1 + w_H(\mathbf{u}) \pmod 2 + \widetilde{f}(\mathbf{u})$ is identically null on $\{\mathbf{u} \in \mathbb{F}_2^n \mid \mathbf{u} \preceq \mathbf{y}\}$.

Summarizing, we have:

(i) if $w_H(\mathbf{y}) < n/2$, then $f(\mathbf{y}) = 0$ and $\sum_{\mathbf{u} \preceq \overline{\mathbf{y}}} (-1)^{\widetilde{f}(\mathbf{u})} = 2^{n/2}$;

(ii) if $w_H(\mathbf{y}) > n/2$, then $f(\mathbf{y}) = 1$ and $\sum_{\mathbf{u} \preceq \mathbf{y}} (-1)^{1+w_H(\mathbf{u})+\widetilde{f}(\mathbf{u})} = 2^{n/2}$;

(iii) if $w_H(\mathbf{y}) = n/2$, when $f(\mathbf{y}) = 0$, then $\widetilde{f}$ is identically null on $\{\mathbf{u} \in \mathbb{F}_2^n \mid \mathbf{u} \preceq \overline{\mathbf{y}}\}$ and, when $f(\mathbf{y}) = 1$, then $1 + w_H(\mathbf{u}) \pmod 2 + \widetilde{f}(\mathbf{u})$ is identically null on $\{\mathbf{u} \in \mathbb{F}_2^n \mid \mathbf{u} \preceq \mathbf{y}\}$.

Condition (iii) implies that an element $\mathbf{y}$ of Hamming weight $n/2$ in the support of f and an element $\mathbf{y}'$ of Hamming weight $n/2$ whose complement is outside the support of f are necessarily such that the set

$$\{\mathbf{u} \in \mathbb{F}_2^n \mid \mathbf{u} \preceq \mathbf{y} \text{ and } \mathbf{u} \preceq \mathbf{y}'\}$$

contains no element of even Hamming weight, which is impossible since this set contains the zero vector. This means that either all elements of Hamming weight $n/2$ are in the support of f or all are outside. In both cases, we arrive at a contradiction since the majority function is not bent for $n \geq 4$. □

Remark 4.2. For $n = 2$, two monotone bent functions exist, namely, the strict and large majority functions, whose supports are the sets $\{(1, 1)\}$ and $\{(0, 1), (1, 0), (1, 1)\}$ (recall that a function in two variables is bent if and only if it has odd Hamming weight).

4.2 Homogeneous monotone functions

A Boolean function is called *homogeneous* if all the monomials in its ANF have the same degree.

Monotone homogeneous functions exist (the simplest ones are the monomials; the simplest polynomial one, in three variables, is $\mathbf{x}_1\mathbf{x}_2 + \mathbf{x}_1\mathbf{x}_3 + \mathbf{x}_2\mathbf{x}_3$).

Theorem 3.1 can be specified to give a secondary construction of homogeneous monotone functions, but the hypothesis is then rather restrictive:

- If $f \in \mathcal{B}_n$ is monotone homogeneous, and
- $g_1, \ldots, g_n \in \mathcal{B}_m$ are n monotone homogeneous functions, each of distinct variables, which all have the same degree,

then the vectorial composition $f \circ \mathbf{g} \in \mathcal{B}_{mn}$ is monotone homogeneous, where $\mathbf{g} = (g_1, \ldots, g_n)$.

Corollary 3.2 also gives a secondary construction of homogeneous monotone functions, but a rather straightforward one:

If f is homogeneous monotone, then the function obtained by replacing any monomial $\mathbf{x}^{\mathbf{v}}$ by $\mathbf{x}^{\mathbf{v}}\mathbf{y}^{\mathbf{v}}\mathbf{z}^{\mathbf{v}} \ldots$ (that is, replacing each x_i by $x_i y_i z_i \ldots$) in the ANF of f is homogeneous monotone as well. This is generalized below in Theorem 4.5 (B).

Homogeneous monotone functions have the following nice property.

Lemma 4.3. *Let*

$$f(\mathbf{x}) = \sum_{\mathbf{v} \in A} \mathbf{x}^{\mathbf{v}}$$

be a homogeneous function, where all the elements in A have Hamming weight d. Assume that f is monotone. Then the least vector support Γ of f equals A.

Proof. For any $\mathbf{v} \in A$, we have $f(\mathbf{v}) = 1$, since $\mathbf{v}^{\mathbf{v}} = 1$ and $\mathbf{v}^{\mathbf{v}'} = 0$ for every other $\mathbf{v}'$ in A, because some index i exists in the support of $\mathbf{v}'$ such that the corresponding coordinate of $\mathbf{v}$ is null. And for every $\mathbf{v}'$ in $\mathbb{F}_2^n$ such that $\mathbf{v}' \prec \mathbf{v}$ we have $f(\mathbf{v}') = 0$. Thus, $\mathbf{v} \in \Gamma$. Let now $\mathbf{v} \notin A$ be given with $f(\mathbf{v}) = 1$. It follows that $|\mathrm{supp}(\mathbf{v})| > d$, since otherwise, for every $\mathbf{v}' \in A$, some index i exists in the support of $\mathbf{v}'$ such that the corresponding coordinate of $\mathbf{v}$ is null. Furthermore, there exists $\mathbf{v}_0$ with $\mathbf{v}_0 \preceq \mathbf{v}$, such that $\mathrm{supp}(\mathbf{v}_0) \in A$, and so $\mathbf{v}$ is not a least vector in the support of f. □

The following lemma (whose proof is rather straightforward) proves to be quite useful.

Lemma 4.4. *A homogeneous function $\sum_{\mathbf{v} \in \Gamma} \mathbf{x}^{\mathbf{v}}$ is monotone if and only if for each $\mathbf{x} \in \mathbb{F}_2^n$, for which there exists $\mathbf{v} \in \Gamma$ such that $\mathbf{v} \preceq \mathbf{x}$, the number of such $\mathbf{v}$ is odd.*

We next make some observations, find a construction for homogeneous monotone functions based upon Corollary 3.3 (Construction MBF), and we further prove a nonexistence result, under some restrictive conditions.

Theorem 4.5. (A) *If f is a homogeneous monotone Boolean function, then:*

(i) $m = |\Gamma|$ *is odd.*

(ii) *We have* $1 + \prod_{\mathbf{v}\in\Gamma}(1 + \mathbf{x}^{\mathbf{v}}) = \sum_{\mathbf{v}\in\Gamma} \mathbf{x}^{\mathbf{v}}$, *over* $\mathbb{F}_2$.

(iii) *For every non-zero* $\mathbf{u} \in \mathbb{F}_2^n$,

$$\sum_{k=1}^{m} (2^k(-1)^{m-k} + 2(-1)^k)\left|\{(i_1, \ldots, i_k) \subseteq \{1, \ldots, m\} \mid \mathbf{v}_{i_1 \ldots i_k} = \mathbf{u}\}\right| = 0.$$

(B) *(Construction HMBF) If* $f_i(\mathbf{x}) = \sum_{\mathbf{v}\in\Gamma_i} \mathbf{x}^{\mathbf{v}}$ *for* $i = 1, \ldots, k$ *are monotone homogeneous functions with* $\Gamma_i = \{\mathbf{v}_{ij}\}_{j=1}^m$ *and* $|\Gamma_i| = m$, *then the function*

$$\hat{f}(\mathbf{x}_1, \ldots, \mathbf{x}_k) = \sum_{i=1}^{m} \prod_{j=1}^{k} \mathbf{x}_j^{\mathbf{v}_{ij}}; \quad \mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbb{F}_2^n$$

is also monotone homogeneous in $\mathcal{B}_{kn}$ *of least vector support* $\hat{\Gamma} = \{(\mathbf{v}_{1j}, \ldots, \mathbf{v}_{kj})_{j=1,\ldots,m}\}$.

Proof. The claims (i) and (ii) of (A) follow easily from the above lemmas and/or Theorem 2.1. Regarding claim (iii), we observe that the identity $\sum_{\mathbf{v}\in\Gamma}(1 + \mathbf{x}^{\mathbf{v}}) = \prod_{\mathbf{v}\in\Gamma}(1 + \mathbf{x}^{\mathbf{v}})$ can be transformed into an equality over the ring of integers by using $(-1)^{\sum_{\mathbf{v}\in\Gamma}(1+\mathbf{x}^{\mathbf{v}})} = \prod_{\mathbf{v}\in\Gamma}(2\mathbf{x}^{\mathbf{v}} - 1) = 1 - 2\prod_{\mathbf{v}\in\Gamma}(1 - \mathbf{x}^{\mathbf{v}})$. Expanding and identifying the coefficients, we obtain the claim (iii).

Next, we show our construction for homogeneous monotone Boolean functions, that is, claim (B). It is easy to see that $\hat{f}$ is homogeneous, since, for j fixed, $\mathbf{x}_j^{\mathbf{v}_{ij}}$ has the same degree for every i, and so, $\prod_{j=1}^k \mathbf{x}_j^{\mathbf{v}_{ij}}$ will have the same degree for every i.

To show that $\hat{f}$ is monotone, we use Lemma 4.4. Let $(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k)$ be an arbitrary vector and assume that there exists $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k) \preceq (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k)$. By absurd, we assume that there are an even number of such $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$. Since $\mathbf{v}_1 \preceq \mathbf{x}_1, \mathbf{v}_2 \preceq \mathbf{x}_2$, etc., it follows that there is an index $1 \le i \le k$ such that there are an even number of $\mathbf{v}$ with $\mathbf{v} \preceq \mathbf{x}_i$, which is a contradiction. □

As in Corollary 3.3 (Construction MBF), as a particular case, we can take all f_i $(1 \le i \le k)$ to be equal to a monotone function f (depending on independent sets of variables), of permuted least vector support Γ, then $\hat{f}(\mathbf{x}_1, \ldots, \mathbf{x}_k) = \sum_{i=1}^g \prod_{j=1}^k \mathbf{x}_j^{\mathbf{v}_{\sigma_j(i)}}$ is a monotone and homogeneous Boolean function. Further instantiating, by taking every permutation to be the identity, if $f(\mathbf{x}) = \sum_{\mathbf{v}\in\Gamma} \mathbf{x}^{\mathbf{v}}$ is a monotone homogeneous function, then the function $\hat{f}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \ldots) = \sum_{\mathbf{v}\in\Gamma} \mathbf{x}^{\mathbf{v}}\mathbf{y}^{\mathbf{v}}\mathbf{z}^{\mathbf{v}} \ldots$ is also monotone homogeneous as we already observed.

Note that Remark 2.4 can be obtained by the construction of Theorem 4.5 (B), via an appropriate relabeling, namely $(x_1, x_2, x_3, x_4, x_5, x_6) \leftrightarrow (x_1, y_1, x_2, y_2, x_3, y_3)$. That is, if we take the homogeneous monotone function

$$f(\mathbf{x}) = x_1x_2 + x_1x_3 + x_2x_3$$

with $\Gamma = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$, the homogeneous monotone function of Remark 2.4 is $\hat{f}(\mathbf{x}, \mathbf{y})$, whose least vector support is $\hat{\Gamma} = \{(1, 1, 0, 1, 1, 0), (1, 0, 1, 1, 0, 1), (0, 1, 1, 0, 1, 1)\}$.

We are not aware of any other general construction for homogeneous monotone Boolean functions. It seems difficult to determine all homogeneous monotone functions and we leave this as an open problem.

5 On the nonlinearity of monotone functions

Let f be any n-variable monotone Boolean function. For every $\mathbf{y} \in \mathbb{F}_2^n$ such that $f(\mathbf{y}) = 0$, we have (according to the Poisson summation formula and similarly to what is done in Section 4 above for bent functions)

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n;\, \mathbf{u}\preceq\overline{\mathbf{y}}} W_f(\mathbf{u}) = 2^{n-w_H(\mathbf{y})} \sum_{\mathbf{x}\in\mathbb{F}_2^n;\, \mathbf{x}\preceq\mathbf{y}} (-1)^{f(\mathbf{x})} = 2^n.$$

This implies that $\max_{\mathbf{u}\in\mathbb{F}_2^n;\,\mathbf{u}\preceq\overline{\mathbf{y}}}|W_f(\mathbf{u})| \geq 2^{w_H(\mathbf{y})}$. For every $\mathbf{y}\in\mathbb{F}_2^n$ such that $f(\mathbf{y})=1$, we have, by applying the Poisson summation formula to the function $f(\overline{\mathbf{x}})$, whose Walsh transform equals $(-1)^{(1,\ldots,1)\cdot\mathbf{u}}W_f(\mathbf{u})$:

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n;\,\mathbf{u}\preceq\mathbf{y}}(-1)^{(1,\ldots,1)\cdot\mathbf{u}}W_f(\mathbf{u}) = 2^{w_H(\mathbf{y})}\sum_{\mathbf{x}\in\mathbb{F}_2^n;\,\mathbf{x}\preceq\overline{\mathbf{y}}}(-1)^{f(\overline{\mathbf{x}})} = 2^{w_H(\mathbf{y})}\sum_{\mathbf{x}\in\mathbb{F}_2^n;\,\mathbf{y}\preceq\mathbf{x}}(-1)^{f(\mathbf{x})} = -2^n.$$

This implies that $\max_{\mathbf{u}\in\mathbb{F}_2^n;\,\mathbf{u}\preceq\mathbf{y}}|W_f(\mathbf{u})| \geq 2^{n-w_H(\mathbf{y})}$.

If $f(\mathbf{x})$ differs from the majority function for at least one input $\mathbf{x}$ of Hamming weight different from $n/2$, then there exists $\mathbf{y}$ either of Hamming weight larger than $n/2$ and such that $f(\mathbf{y})=0$ or of Hamming weight smaller than $n/2$ and such that $f(\mathbf{y})=1$. In both cases we have $\max_{\mathbf{u}\in\mathbb{F}_2^n}|W_f(\mathbf{u})| \geq 2^{n/2+1}$ if n is even and $\max_{\mathbf{u}\in\mathbb{F}_2^n}|W_f(\mathbf{u})| \geq 2^{(n+1)/2}$ if n is odd, and then

$$\mathrm{nl}(f) \leq \begin{cases} 2^{n-1}-2^{n/2} & \text{if } n \text{ is even,}\\ 2^{n-1}-2^{(n-1)/2} & \text{if } n \text{ is odd.}\end{cases}$$

If $f(\mathbf{x})$ does not differ from the majority function for at least one input $\mathbf{x}$ of Hamming weight different from $n/2$, then, if n is odd then f is the majority function and we know that this same inequality $\mathrm{nl}(f)\leq 2^{n-1}-2^{(n-1)/2}$ is true for $n\geq 5$ since the nonlinearity equals $2^{n-1}-\binom{n-1}{(n-1)/2}$. We deduce:

Theorem 5.1. *Let $n\geq 5$ be odd and $f\in\mathcal{B}_n$ be monotone. Then* $\mathrm{nl}(f)\leq 2^{n-1}-2^{(n-1)/2}$.

We conjecture that, if n is even and sufficiently large, then

$$\mathrm{nl}(f)\leq 2^{n-1}-2^{n/2}.$$

Observe that this conjecture, if true, provides an alternative proof of our main result, at least for large n.

6 Algebraic immunity of monotone Boolean functions

We next are concerned with the algebraic immunity of monotone functions.

Theorem 6.1. *The algebraic immunity of a monotone Boolean function f is*

$$\mathcal{AI}(f)\leq \min\{\lceil n/2\rceil, \min_{\mathbf{v}\in\Gamma}\{w_H(\mathbf{v})\}, \min_{\mathbf{v}\in F}\{n-w_H(\mathbf{v})\}\}, \tag{6.1}$$

where F is constituted by all vectors in $\mathbb{F}_2^n\setminus\mathrm{supp}(f)$ that are greatest in the partial ordering $\preceq$.

Proof. Firstly, we simply observe that

$$(f+1)\,\mathbf{x}^{\mathbf{w}} = \mathbf{x}^{\mathbf{w}}\prod_{\mathbf{v}\in\Gamma}(1+\mathbf{x}^{\mathbf{v}}) = 0,$$

for any $\mathbf{w}\in\Gamma$, and so a minimal annihilator of $f+1$ is given by $\mathbf{x}^{\mathbf{v}_0}$, where $\mathbf{v}_0$ has minimal weight (not unique, in general). Using [5], we have

$$\mathcal{AI}(f)\leq \min\{\lceil n/2\rceil, \min_{\mathbf{v}\in\Gamma}\{w_H(\mathbf{v})\}\}.$$

Further, note that for any $\mathbf{w}\in F$ we have

$$f(\mathbf{x})\,\overline{\mathbf{x}}^{\overline{\mathbf{w}}} = f(\mathbf{x})\prod_{i\in\mathrm{supp}(\overline{\mathbf{w}})}(1+x_i) = 0,$$

since $\overline{\mathbf{x}}^{\overline{\mathbf{w}'}}=1$ if and only if $\mathbf{w}'\preceq\mathbf{w}$ and since $f(\mathbf{w}')=0$ for any $\mathbf{w}'\preceq\mathbf{w}$. Thus, we have

$$\mathcal{AI}(f)\leq \min_{\mathbf{w}\in F}\{n-w_H(\mathbf{w})\},$$

thanks to $\deg(\overline{\mathbf{x}}^{\overline{\mathbf{w}}}) = |\mathrm{supp}(\overline{\mathbf{w}})|$.

From what has been discussed above, we immediately get our assertion. □

Inequality (6.1) is certainly attained (take as an example the majority function, for even n), but in general, it is strict. For instance, if we take $n = 6$ and the least support $\Gamma = \{\mathbf{v} = (1, 1, 1, 0, 0, 0), \mathbf{w} = (0, 0, 0, 1, 1, 1)\}$, then the monotone function

$$f(\mathbf{x}) = 1 + (1 + \mathbf{x}^{\mathbf{v}})(1 + \mathbf{x}^{\mathbf{w}}) = 1 + (1 + x_1x_2x_3)(1 + x_4x_5x_6) = x_1x_2x_3 + x_4x_5x_6 + x_1x_2x_3x_4x_5x_6$$

has algebraic immunity 2, as one can easily check, and $\min_{\mathbf{v}\in\Gamma}\{w_H(\mathbf{v})\} = 3$.
We can certainly give a sufficient criterion for a more precise result (albeit, a weak result from a cryptographic viewpoint).

Proposition 6.2. *Let f be a monotone Boolean function whose least vector support is $\Gamma = \{\mathbf{v}_1, \ldots, \mathbf{v}_g\}$. If $\bigcap_{\mathbf{v}\in\Gamma} \mathrm{supp}(\mathbf{v}) \neq \emptyset$, then the algebraic immunity of f is $\mathcal{AI}(f) = 1$.*

Proof. Write $f(\mathbf{x}) = \sum_{\mathbf{w}\in A} \mathbf{x}^{\mathbf{w}}$, for some set of vectors A. Since $\bigcap_{\mathbf{v}\in\Gamma} \mathrm{supp}(\mathbf{v}) \neq \emptyset$, there exists $i_0 \in \bigcap_{\mathbf{v}\in\Gamma} \mathrm{supp}(\mathbf{v})$, and so, $i_0 \in \bigcap_{\mathbf{w}\in A} \mathrm{supp}(\mathbf{w})$ as well. Thus

$$f(\mathbf{x}) \cdot (1 + x_{i_0}) = \sum_{\mathbf{w}\in A} \mathbf{x}^{\mathbf{w}} + \sum_{\mathbf{w}\in A} \mathbf{x}^{\mathbf{w}} = 0,$$

which shows that $\mathcal{AI}(f) = 1$ (since it is obvious from our condition that f is not constant). □

Example 6.3. Let $n = 5$ and $\Gamma = \{\mathbf{v} = (1, 0, 1, 1, 0), \mathbf{w} = (0, 1, 0, 1, 1)\}$. Then the monotone Boolean function

$$f(\mathbf{x}) = 1 + (1 + \mathbf{x}^{\mathbf{v}})(1 + \mathbf{x}^{\mathbf{w}}) = 1 + (1 + x_1x_3x_4)(1 + x_2x_4x_5) = x_1x_3x_4 + x_2x_4x_5 + x_1x_2x_3x_4x_5$$

has $\mathcal{AI}(f) = 1$, since $1 + x_4$ is an annihilator of f.

From a cryptographic viewpoint, we are interested in those monotone functions which have maximum algebraic immunity. For an odd number of variables n, Qu, Li and Feng proved in [15] that there are exact two n-variable symmetric Boolean functions with maximum algebraic immunity, the majority function and its complement. For an even number of variables n, Peng, Wu and Kan [14] determined all the symmetric Boolean functions with maximum algebraic immunity; the total number of such symmetric Boolean functions is $(2w_H(n) + 1)2^{\lfloor \log_2 n \rfloor}$, where $w_H(n)$ is the Hamming weight of the binary expansion of n. It would be interesting to determine the exact number of monotone functions with maximum algebraic immunity, and we shall do that next.

First, for any even $n \geq 4$, we define a function $f \in \mathcal{B}_n$ as

$$f(\mathbf{x}) = \begin{cases} 0, & \text{if } w_H(\mathbf{x}) < \frac{n}{2}, \\ b_{\mathbf{x}} & \text{if } w_H(\mathbf{x}) = \frac{n}{2}, \\ 1, & \text{if } w_H(\mathbf{x}) > \frac{n}{2}, \end{cases} \tag{6.2}$$

where $b_{\mathbf{x}}$ can be taken arbitrarily in $\mathbb{F}_2$. Let us denote by $\mathcal{B}'_n$ the set of all Boolean functions given by (6.2). It has been proved in [8] that every function in $\mathcal{B}'_n$ has maximum algebraic immunity. We can easily see that every function in $\mathcal{B}'_n$ is monotone.

Theorem 6.4. *For every odd n, the majority function of n variables is the unique monotone function with maximum algebraic immunity. For every even $n \geq 4$, a monotone function $f \in \mathcal{B}_n$ has maximum algebraic immunity if and only if $f \in \mathcal{B}'_n$. The number of such monotone Boolean functions on even $n \geq 4$ number of variables is $2^{\binom{n}{n/2}}$, among which there are*

$$\binom{\binom{n}{n/2}}{\frac{1}{2}\binom{n}{n/2}}$$

balanced ones.

Proof. It is well known that if a function in odd number of variables has maximum algebraic immunity then it is balanced. By Theorem 6.1, we directly get our first claim, since Γ can then only contain vectors of weights larger than or equal to $\lceil n/2 \rceil$ and, the function being balanced, Γ must then equal the set of all vectors of such weight.

To show the second claim, recall that every function in $\mathcal{B}'_n$ has maximum algebraic immunity. Thus if $f \in \mathcal{B}'_n$, we have that f has maximum algebraic immunity. We now prove that if f has maximum algebraic immunity then $f \in \mathcal{B}'_n$. According to Theorem 6.1, if f has maximum algebraic immunity $n/2$, then any element of the least support set of f has Hamming weight no less than $n/2$ and every element in $_F$ has Hamming weight strictly less than $n/2 + 1$. This implies that $f \in \mathcal{B}'_n$. Certainly, the count follows easily from (6.2), and so, for every even $n \geq 4$, there are exactly $2^{\binom{n}{n/2}}$ monotone functions with maximum algebraic immunity, and, among these there are exact

$$\binom{\binom{n}{n/2}}{\frac{1}{2}\binom{n}{n/2}}$$

balanced such functions. □

7 Walsh spectrum of monotone Boolean functions

Recall the notation for the subspace $E_{i_1,\dots,i_k}$ of vectors "disjoint" from $\bigvee_{j=1}^{k} \mathbf{v}_{i_j}$ in (1.2).

For any subspace $E \subset \mathbb{F}_2^n$, let $E^\perp$ denote the algebraic dual space of E. The following useful fact will not be proven here.

Lemma 7.1 ("character-sum property" [1]). *If E is any $\mathbb{F}_2$-subspace of $\mathbb{F}_2^n$ and $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ then*

$$\sum_{\mathbf{x} \in \mathbf{b}+E} (-1)^{\mathbf{a}\cdot\mathbf{x}} = \begin{cases} |E|(-1)^{\mathbf{a}\cdot\mathbf{b}}, & \mathbf{a} \in E^\perp, \\ 0, & \mathbf{a} \notin E^\perp. \end{cases}$$

We next look at the Walsh–Hadamard spectrum of a monotone Boolean function $f(\mathbf{x}) = 1 + \prod_{\mathbf{v}\in\Gamma}(1 + \mathbf{x}^{\mathbf{v}})$.

Theorem 7.2. *Let f be a nonconstant monotone Boolean function with least vector support Γ.*

(i) *If $|\Gamma| = 1$ (i.e., f is atomic), say $\Gamma = \{\mathbf{v}\}$, then the Walsh–Hadamard spectrum of f is*

$$W_f(\mathbf{u}) = \begin{cases} 2^n - 2^{n+1-w_H(\mathbf{v})} & \text{for } \mathbf{u} = \mathbf{0}, \\ 2^{n+1-w_H(\mathbf{v})}(-1)^{1+\mathbf{u}\cdot\mathbf{v}} & \text{for } \mathbf{u} \neq \mathbf{0}. \end{cases}$$

Consequently, the nonlinearity is $\mathrm{nl}(f) = 0$ if $w_H(\mathbf{v}) = 1$, or $\mathrm{nl}(f) = 2^{n-w_H(\mathbf{v})}$ if $w_H(\mathbf{v}) > 1$.

(ii) *If $|\Gamma| = 2$, say $\Gamma = \{\mathbf{v}_1, \mathbf{v}_2\}$, then the Walsh–Hadamard spectrum of f is*

$$W_f(\mathbf{u}) = \begin{cases} 2^n - 2^{n+1-w_H(\mathbf{v}_1)} - 2^{n+1-w_H(\mathbf{v}_2)} + 2^{n+1-w_H(\mathbf{v}_1\vee\mathbf{v}_2)} & \text{for } \mathbf{u} = \mathbf{0}, \\ 2^{n+1-w_H(\mathbf{v}_1)}(-1)^{1+\mathbf{u}\cdot\mathbf{v}_1}\delta_{E_1^\perp}(\mathbf{u}) + 2^{n+1-w_H(\mathbf{v}_2)}(-1)^{1+\mathbf{u}\cdot\mathbf{v}_2}\delta_{E_2^\perp}(\mathbf{u}) & \\ \quad - 2^{n+1-w_H(\mathbf{v}_1\vee\mathbf{v}_2)}(-1)^{1+\mathbf{u}\cdot(\mathbf{v}_1\vee\mathbf{v}_2)}\delta_{E_{12}^\perp}(\mathbf{u}) & \text{for } \mathbf{u} \neq \mathbf{0}. \end{cases}$$

(iii) *In general, the Walsh spectrum for a monotone f with $\Gamma = \{\mathbf{v}_1, \dots, \mathbf{v}_g\}$ is*

$$W_f(\mathbf{u}) = \begin{cases} 2^n - 2^{n+1}\sum_{k=1}^{g}(-1)^{k-1}\sum_{1\leq i_1<\cdots<i_k\leq g} 2^{-w_H(\mathbf{v}_{i_1 i_2 \dots i_k})} & \text{for } \mathbf{u} = \mathbf{0}, \\ 2^{n+1}\sum_{k=1}^{g}\sum_{1\leq i_1<\cdots<i_k\leq g} 2^{-w_H(\mathbf{v}_{i_1 i_2\dots i_k})}(-1)^{k+\mathbf{u}\cdot\mathbf{v}_{i_1 i_2\dots i_k}}\delta_{E^\perp_{i_1 i_2\dots i_k}}(\mathbf{u}) & \text{for } \mathbf{u} \neq \mathbf{0}. \end{cases}$$

Proof. First, observe that the Walsh–Hadamard transform of f is

$$\begin{aligned} W_f(\mathbf{u}) &= 2^n\delta(\mathbf{u}) - 2\sum_{\mathbf{x}\in\mathbb{F}_2^n} f(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^n\delta(\mathbf{u}) - 2\sum_{\mathbf{x}\in\mathrm{supp}(f)} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= 2^n\delta(\mathbf{u}) - 2\sum_{\substack{\mathbf{x}\in\mathbb{F}_2^n, \mathbf{v}\preceq\mathbf{x} \\ \text{for some } \mathbf{v}\in\Gamma}} (-1)^{\mathbf{u}\cdot\mathbf{x}}. \end{aligned}$$

Assume first that $\Gamma = \{\mathbf{v}\}$ ($\mathbf{v} \neq \mathbf{0}$, since f is nonconstant). We want to point out that variations of this first "atomic" case are known (see, for instance, MacWilliams and Sloane [12, Chapters 13–15]), but we include

the complete argument here, as it will provide some insight into the general case. If $w_H(\mathbf{v}) = 1$, then $f(\mathbf{x}) = \mathbf{x}^{\mathbf{v}}$ ($= x_i$, where $v_i \neq 0$) is certainly linear and the claim regarding the nonlinearity follows immediately, so we assume that $w_H(\mathbf{v}) \geq 2$. Then,

$$W_f(\mathbf{0}) = 2^n - 2\sum_{\mathbf{x}\in\mathbb{F}_2^n, \mathbf{v}\preceq\mathbf{x}} 1 = 2^n - 2\big|\{\mathbf{x}\in\mathbb{F}_2^n \mid \mathbf{v}\preceq\mathbf{x}\}\big| = 2^n - 2^{n+1-w_H(\mathbf{v})}.$$

Next, observe that

$$E = \{\mathbf{u}\in\mathbb{F}_2^n \mid \mathbf{u} * \mathbf{v} = \mathbf{0}\} = \{\mathbf{u}\in\mathbb{F}_2^n \mid \mathrm{supp}(\mathbf{u})\cap\mathrm{supp}(\mathbf{v}) = \emptyset\}$$

is a subspace of $\mathbb{F}_2^n$ of cardinality $|E| = 2^{n-w_H(\mathbf{v})}$, and $\{\mathbf{x}\in\mathbb{F}_2^n \mid \mathbf{v}\preceq\mathbf{x} \text{ for some } \mathbf{v}\in\Gamma\} = \mathbf{v} + E$. Thus, for $\mathbf{u}\neq\mathbf{0}$, using, as before, the character-sum property (Lemma 7.1), we get

$$\begin{aligned} W_f(\mathbf{u}) &= -2\sum_{\mathbf{x}\in\mathbb{F}_2^n, \mathbf{v}\preceq\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} = -2\sum_{\mathbf{x}\in\mathbf{v}+E} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= -2\begin{cases} |E|(-1)^{\mathbf{u}\cdot\mathbf{v}} & \text{if } \mathbf{u}\in E^\perp, \\ 0 & \text{otherwise} \end{cases} = \begin{cases} 2^{n+1-w_H(\mathbf{v})}(-1)^{1+\mathbf{u}\cdot\mathbf{v}} & \text{if } \mathbf{u}\in E^\perp, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

If $w_H(\mathbf{u}) > 1$, then the nonlinearity is

$$\begin{aligned} \mathrm{nl}(f) &= 2^{n-1} - \frac{1}{2}\max_{\mathbf{u}}|W_f(\mathbf{u})| \\ &= 2^{n-1} - \frac{1}{2}\max\{2^n - 2^{n+1-w_H(\mathbf{v})}, 2^{n+1-w_H(\mathbf{v})}\} \\ &= 2^{n-1} - \frac{1}{2}(2^n - 2^{n+1-w_H(\mathbf{v})}) = 2^{n-w_H(\mathbf{v})}. \end{aligned}$$

We next consider the case of $|\Gamma| = 2$, say $\Gamma = \{\mathbf{v}_1, \mathbf{v}_2\}$. As before,

$$\begin{aligned} W_f(\mathbf{0}) &= 2^n - 2\sum_{\substack{\mathbf{x}\in\mathbb{F}_2^n, \mathbf{v}\preceq\mathbf{x} \\ \text{for some } \mathbf{v}\in\Gamma}} 1 \\ &= 2^n - 2\big(\big|\{\mathbf{x}\in\mathbb{F}_2^n \mid \mathbf{v}_1\preceq\mathbf{x}\}\big| + \big|\{\mathbf{x}\in\mathbb{F}_2^n \mid \mathbf{v}_2\preceq\mathbf{x}\}\big| - \big|\{\mathbf{x}\in\mathbb{F}_2^n \mid \mathbf{v}_1\vee\mathbf{v}_2\preceq\mathbf{x}\}\big|\big) \\ &= 2^n - 2^{n+1-w_H(\mathbf{v}_1)} - 2^{n+1-w_H(\mathbf{v}_2)} + 2^{n+1-w_H(\mathbf{v}_1\vee\mathbf{v}_2)}. \end{aligned}$$

Let $E_i = \{\mathbf{u}\in\mathbb{F}_2^n \mid \mathbf{u} * \mathbf{v}_i = \mathbf{0}\}$ for $i = 1, 2$, and $E_{12} = \{\mathbf{u}\in\mathbb{F}_2^n \mid \mathbf{u} * (\mathbf{v}_1\vee\mathbf{v}_2) = \mathbf{0}\}$. Then[2] we have,

$$\begin{aligned} W_f(\mathbf{u}) &= -2\sum_{\substack{\mathbf{x}\in\mathbb{F}_2^n, \mathbf{v}\preceq\mathbf{x} \\ \text{for some } \mathbf{v}\in\Gamma}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= -2\Big(\sum_{\mathbf{x}\in\mathbf{v}_1+E_1}(-1)^{\mathbf{u}\cdot\mathbf{x}} + \sum_{\mathbf{x}\in\mathbf{v}_2+E_2}(-1)^{\mathbf{u}\cdot\mathbf{x}} - \sum_{\mathbf{x}\in\mathbf{v}_1\vee\mathbf{v}_2+E_{12}}(-1)^{\mathbf{u}\cdot\mathbf{x}}\Big) \\ &= -2|E_1|(-1)^{\mathbf{u}\cdot\mathbf{v}_1}\delta_{E_1^\perp}(\mathbf{u}) + |E_2|(-1)^{\mathbf{u}\cdot\mathbf{v}_2}\delta_{E_2^\perp}(\mathbf{u}) - |E_{12}^*|(-1)^{\mathbf{u}\cdot(\mathbf{v}_1\vee\mathbf{v}_2)}\delta_{E_{12}^\perp}(\mathbf{u}) \\ &= 2^{n+1-w_H(\mathbf{v}_1)}(-1)^{1+\mathbf{u}\cdot\mathbf{v}_1}\delta_{E_1^\perp}(\mathbf{u}) + 2^{n+1-w_H(\mathbf{v}_2)}(-1)^{1+\mathbf{u}\cdot\mathbf{v}_2}\delta_{E_2^\perp}(\mathbf{u}) \\ &\quad - 2^{n+1-w_H(\mathbf{v}_1\vee\mathbf{v}_2)}(-1)^{1+\mathbf{u}\cdot(\mathbf{v}_1\vee\mathbf{v}_2)}\delta_{E_{12}^\perp}(\mathbf{u}). \end{aligned}$$

Certainly, the method can be extended to arbitrary $\Gamma = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$, using the inclusion-exclusion principle. Recall that $\mathbf{v}_{i_1 i_2 \ldots i_k} = \bigvee_{j=1}^k \mathbf{v}_{i_j}$, and

$$E_{i_1 i_2 \ldots i_k} = \{\mathbf{u}\in\mathbb{F}_2^n \mid \mathbf{u} * \mathbf{v}_{i_1 i_2 \ldots i_k} = \mathbf{0}\}.$$

With these notations, we obtain

$$\begin{aligned} W_f(\mathbf{0}) &= 2^n - 2^{n+1}\sum_{k=1}^m (-1)^{k-1}\sum_{1\leq i_1<\cdots<i_k\leq m} 2^{-w_H(\mathbf{v}_{i_1 i_2 \ldots i_k})}, \\ W_f(\mathbf{u}) &= 2^{n+1}\sum_{k=1}^m \sum_{1\leq i_1<\cdots<i_k\leq m} 2^{-w_H(\mathbf{v}_{i_1 i_2 \ldots i_k})}(-1)^{k+\mathbf{u}\cdot\mathbf{v}_{i_1 i_2 \ldots i_k}}\delta_{E_{i_1 i_2 \ldots i_k}^\perp}(\mathbf{u}) \quad \text{for } \mathbf{u}\neq 0. \end{aligned}$$

□

2 Recall the notation for the Kronecker delta function $\delta_S(\mathbf{u}) = 1$ if $\mathbf{u}\in S$, and 0 otherwise.

Next, we make some observations on the property of being balanced, for an n-variable monotone Boolean function of least support set $\Gamma = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$. For easy writing, we introduce the notation

$$w_{i_1 i_2 \ldots i_s} = w_H(\mathbf{v}_{i_1 i_2 \ldots i_s}),$$

and assume without loss of generality that $w_1 \le w_2 \le \cdots \le w_m$.

It is known that a Boolean function f is balanced if and only if $W_f(\mathbf{0}) = 0$. Thus, by the previous theorem, f is a balanced monotone function of least support $\Gamma = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ if and only if

$$\sum_{k=1}^{m} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le m} 2^{-w_H(\mathbf{v}_{i_1 i_2 \ldots i_k})} = 2^{-1}.$$

When $|\Gamma| = 1$ is straightforward, every monotone function is a singleton, say x_i, and these are obviously balanced. If $|\Gamma| = 2$, say $\Gamma = \{\mathbf{v}_1, \mathbf{v}_2\}$ (of weights $w_i = w_H(\mathbf{v}_i)$, $i = 1, 2$, and $w_{12} = w_H(\mathbf{v}_{12})$, assuming, without loss of generality, that $w_1 \le w_2$) then f is balanced if and only if $W_f(\mathbf{0}) = 0$, which is equivalent to

$$2^{-w_1} + 2^{-w_2} = 2^{-1} + 2^{-w_{12}}.$$

Multiplying by $2^{w_{12}}$ throughout, we get

$$2^{w_{12}-w_1} + 2^{w_{12}-w_2} = 2^{w_{12}-1} + 1,$$

where $0 \le w_{12} - w_1 \le w_{12} - w_2 \le w_{12} - 1$. By the uniqueness of binary representations, we get $w_{12} = w_2$ and $w_1 = 1$, which contradicts $w_1 < w_{12}$ (in general, since the $\mathbf{v}_i$ are minimal in our partial order, it follows that $w_i < w_{i_1 \ldots i \ldots i_s}$, for any $i_1 < \cdots < i < \cdots < i_s$, $s > 1$). Thus, there are no balanced monotone functions with $|\Gamma| = 2$.

In general, if a monotone f with $\Gamma = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ ($m \ge 3$) as its least support is balanced then

$$\sum_{\substack{1 \le i_1 < \cdots < i_k \le m \\ 1 \le k \le m, \text{ odd}}} 2^{-w_{i_1 \ldots i_k}} = \sum_{\substack{1 \le i_1 < \cdots < i_k \le m \\ 0 \le k \le m, \text{ even}}} 2^{-w_{i_1 \ldots i_k}} \tag{7.1}$$

(by convention, $w_{i_1 \ldots i_k} = 1$ if $k = 0$).

One can show easily that the sets of exponents in the two sides of (7.1) cannot be the same. If they were, the smallest exponent (in absolute value) in the right-hand side of (7.1) is w_1, and the smallest element (in absolute value) in the left-hand side of (7.1) is 1, and so, they must be equal, that is, $w_1 = 1$. Further, it follows from (7.1) that there exist $i_1 < \cdots < i_{2s}$ such that $w_2 = w_{i_1 i_2 \ldots i_{2s}}$. Since $w_2 < w_{j_1 j_2 \ldots j_t}$, if 2 occurs among the indices $j_1 < j_2 < \cdots < j_t$ ($t \ge 2$), it follows that none of the indices $i_1, i_2, \ldots, i_{2s}$ happens to be 2. Since $s \ge 1$, then $i_2 > 2$, and so $w_{i_1 i_2 \ldots i_{2s}} > w_{i_2} \ge w_2$, which is a contradiction.

Remark 7.3. From Theorem 7.2 (i) we easily infer [4, Theorem 3.6] where it was shown that the Cayley graph (undirected graph having $\mathbb{F}_2^n$ as vertices, and $\{\mathbf{u}, \mathbf{v}\}$ as edges, where $\mathbf{u} + \mathbf{v} \in \mathrm{supp}(f)$) of an atomic monotone function (that is, the least vector support Γ has cardinality 1) is singular (which is equivalent to the existence of a zero Walsh coefficient) if and only if the weight of f is even.

Acknowledgment: We thank the anonymous referees for their helpful discussions, in particular pointing out an error in an earlier version of the paper. We thank Charles Celerier and Caroline Melles for useful discussions. Part of this paper was started during an enjoyable visit of the third author at the Naval Academy in Annapolis. The second and third named authors thank this institution for the excellent working conditions.

References

[1] C. Carlet, Two new classes of bent functions, in: *Advances in Cryptology* (Eurocrypt 1993), Lecture Notes in Comput. Sci. 765, Springer, Berlin (1994), 77–101.

[2] C. Carlet, Boolean functions for cryptography and error correcting codes, in: *Boolean Methods and Models*, Cambridge University Press, Cambridge (2010), 257–397.

[3] C. Carlet, Vectorial boolean functions for cryptography, in: *Boolean Methods and Models*, Cambridge University Press, Cambridge (2010), 398–469.

[4] C. Celerier, D. Joyner, C. Melles and D. Phillips, On the Walsh–Hadamard transform of monotone Boolean functions, *Tbilisi Math. J.* **5** (2012), 19–35.

[5] N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, in: *Advances in Cryptology* (Eurocrypt 2003), Lecture Notes in Comput. Sci. 2656, Springer, Berlin (2003), 345–359.

[6] Y. Crama and P. L. Hammer, *Boolean Functions. Theory, Algorithms, and Applications*, Cambridge University Press, Cambridge, 2011.

[7] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, Elsevier/Academic Press, Amsterdam, 2009.

[8] D. K. Dalai, S. Maitra and S. Sarkar, Basic theory in construction of Boolean functions with maximum possible annihilator immunity, *Des. Codes Cryptogr.* **40** (2006), 41–58.

[9] J. F. Dillon, Elementary Hadamard difference sets, in: *Proceedings of the 6th Southeastern Conference on Combinatorics, Graph Theory, and Computing*, Utilitas Mathematica Publishing, Winnipeg (1975), 237–249.

[10] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, in: *Fast Software Encryption* (Leuven 1994), Lecture Notes in Comput. Sci. 1008, Springer, Berlin (1995), 61–74.

[11] R. Fidytek, A. W. Mostowski, R. Somla and A. Szepietowski, Algorithms counting monotone boolean functions, *Information Proc. Lett.* **79** (2001), 203–209.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1977.

[13] W. Meier, E. Pasalic and C. Carlet, Algebraic attacks and decomposition of boolean functions, in: *Advances in Cryptology* (Eurocrypt 2004), Lecture Notes in Comput. Sci. 3027, Springer, Berlin (2004), 474–491.

[14] J. Peng, Q. Wu and H. Kan, On symmetric boolean functions with high algebraic immunity on even number of variables, *IEEE Trans. Inf. Theory* **57** (2011), 7205–7220.

[15] L.-J. Qu, C. Li and K.-Q. Feng, A note on symmetric boolean functions with maximum algebraic immunity in odd number of variables, *IEEE Trans. Inf. Theory* **53** (2007), 2908–2910.

[16] O. S. Rothaus, On bent functions, *J. Combin. Theory Ser. A* **20** (1976), 300–305.